PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-008651
(43)Date of publication of application : 10.01.2003

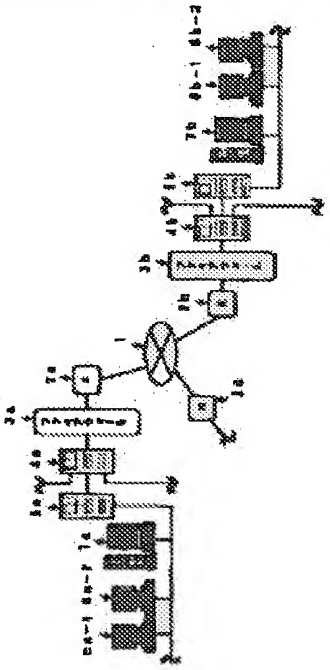
(51)Int.Cl. H04L 12/58
H04L 9/32
H04L 12/66

(21)Application number : 2001-188220
(22)Date of filing : 21.06.2001

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : UENO TOYOSHI

(54) PACKET COMMUNICATION METHOD AND PACKET COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a packet communication method or the like which can oppose wire tapping and other tapping actions done over network lines and even high skillful tapping action done by being intruded into a receiver side server.
SOLUTION: The packet communication method sends and receives packetized communication data through a netted communication network, where the packet communication method extracts an authorized user ID corresponding to a local address, which is one of addresses showing a destination in a header added to the packets and which is an internal address of a local communication network that the destination belongs to, generates a temporary user ID different from the authorized user ID, generates a new header by inserting the temporary user ID into the header that the authorized user ID is extracted from, adds the new header to a data portion of the packet, composes a packet by inserting the extracted authorized user ID into the data portion, and sends the packet composed in the steps above mentioned to the destination.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－8651
（P2003－8651A）
(43)公開日　平成15年１月10日(2003.1.10)

(51)Int.Cl.⁷	識別記号	FI	テーマコード(参考)
H04L 12/58	100	H04L 12/58	100C 5J104
9/32		12/66	B 5K030
12/66		9/00	673A
			673C

審査請求　未請求　請求項の数３　ＯＬ　（全８頁）

(21)出願番号　特願2001－188220(P2001－188220)

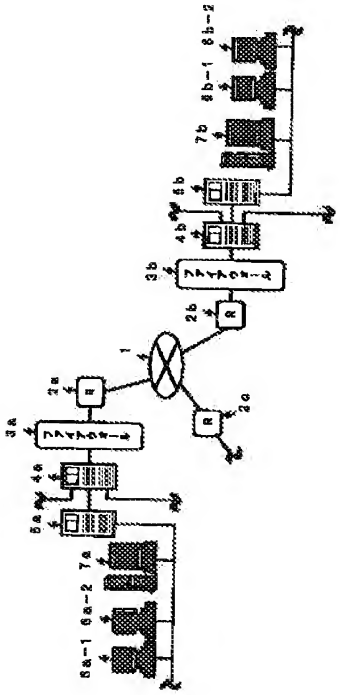
(22)出願日　平成13年６月21日(2001.6.21)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　上野　豊志
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100102439
弁理士　宮田　金雄　（外１名）

最終頁に続く

(54)【発明の名称】　パケット通信方法及びパケット通信システム

(57)【要約】
【課題】　タッピング等のネットワーク経路上において行われる盗聴行為、さらには受信側のサーバに侵入して行われる高度な盗聴行為に対しても有効に対抗し得るパケット通信方法等を提供する。
【解決手段】　網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザＩＤを抽出し、上記正規のユーザＩＤと異なる仮のユーザＩＤを発生し、この仮のユーザＩＤを上記正規のユーザＩＤが抽出されたヘッダ中に挿入して新規のヘッダを生成し、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザＩＤを挿入してパケットを組み立て、上記工程により組み立てられたパケットを送信先に対して送信する。



1

【特許請求の範囲】

【請求項１】　網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザＩＤを抽出する工程と、上記正規のユーザＩＤと異なる任意のユーザＩＤを発生し、この任意のユーザＩＤを上記正規のユーザＩＤが抽出されたヘッダ中に挿入して新規のヘッダを生成する工程と、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザＩＤを挿入してパケットを組み立てる工程と、上記工程により組み立てられたパケットを送信する工程とを備えたことを特徴とするパケット通信方法。

【請求項２】　上記送信パケットに暗号化処理又はスクランブル処理を施したことを特徴とする請求項１記載のパケット通信方法。

【請求項３】　網状の通信ネットワークに接続されたローカル通信ネットワーク内に設けられ、上記通信ネットワークに接続された他のローカル通信ネットワークとの間においてパケット化された通信データを送受信するサーバ装置と、このサーバ装置に接続され、上記サーバ装置に蓄積された自己宛の通信データの取り出し及び上記サーバ装置に対して生成した通信データの送信をそれぞれ行う複数の端末装置と、これら複数の端末装置からそれぞれ送信される通信データのパケットを編集し、そのパケットに付加された送信先の端末装置を示すアドレスのうちローカルアドレスに対応するユーザＩＤをパケット毎に書き替えて上記サーバ装置に出力し、かつ、上記サーバ装置から上記端末装置に取り出される通信データのパケットに付加されたローカルアドレスの識別を行い、自己が属するローカル通信ネットワークのローカルアドレス以外のローカルアドレスが付加されたパケットを蓄積し、蓄積した各パケットから正規のユーザＩＤを抽出したときは抽出した正規のユーザＩＤによりパケットを組立て直して当該ユーザＩＤの端末装置に出力し、上記正規のユーザＩＤを抽出できなかったときは上記蓄積したパケットを破棄するパケット編集手段とを備えたことを特徴とするパケット通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、インターネット等の通信ネットワークを利用して各種データの送受信を行うパケット通信システム及びパケット通信方法に関する。

【０００２】

【従来の技術】近年、コンピュータの普及やインターネット等の社会基盤の整備によりインターネット利用者人口が拡大・増加しており、ＷＷＷ（ワールド・ワイド・

2

ウェブ）、電子メール（Ｅ－ｍａｉｌ）、ＩＰ（インターネット・プロトコル）電話等のインターネットを利用した各種のサービスが提供されている。

【０００３】このうち、電子メールサービスは、インターネットに接続されたメールサーバを介して相手との電子的なメッセージのやりとりを行うものであり、送信側から送信されたメッセージ（以下、送信メールという）は、相手（受信側）が不在の場合でも受信側のメールサーバに蓄積されており、あとで自由に読み出すことができるという特徴がある。ただし、不特定多数の者がアクセス可能なインターネット等の通信ネットワークを介して実現されるため、パケットフィルタリング等のいわゆる盗聴行為により送信メールの内容が他人に覗き見られるという問題があり、送信メールの暗号化やスクランブル等、盗聴行為を防止する各種の対策が行われている。

【０００４】例えば、特開２０００－１８３９６７号公報には、送信パケットのヘッダ内のネットワークアドレス等を書き替えることにより、暗号化やスクランブル等の処理を用いることなくネットワーク経路上における盗聴行為による情報漏洩に対抗することができるパケット通信システムが記載されている。

【０００５】

【発明が解決しようとする課題】しかし、従来のパケット通信システムは、システムの構成上、各パケット通信装置毎に設定されるネットワークアドレスの数が制限されているため、例えば、相手先装置の近傍の１箇所においてタッピングによる盗聴行為が行われ、送信メールの全パケットが捕捉されてしまうと、ネットワークアドレスの同一性を解析されることにより、送信メールの内容が他人に知られてしまうという問題点があった。すなわち、インターネット等における電子メール等の盗聴は、タッピングポイントで収集したパケット群の中から目的のパケットのみを抽出し再組立によって通信内容を盗聴する方式がとられる。

【０００６】また、上述したような暗号化、スクランブル又はネットワークアドレスの書き替え等のいわゆる秘匿処理は、通常、受信側のメールサーバにおいて解除されてしまうため、たとえ送信時に暗号化、スクランブル及びネットワークアドレスの書き替え等の手段が施されていても、このような暗号化等が解除された後を狙った盗聴行為、例えば、受信側メールサーバの処理プログラムを書き替えて受信側のメールサーバに到着した送信メールの内容を盗聴する行為（例えば、目的の送信パケットに記述された送信先アドレスを書き替えて特定のアドレスに転送させるような処理を実行させる場合等）に対しては有効に対抗することができないという問題点があった。

【０００７】この発明は、上記のような課題を解消するためになされたもので、タッピング等のネットワーク経路上において行われる盗聴行為、さらには受信側のサー

3

バに侵入し、受信側サーバの処理プログラムを書き替えて受信側サーバに到着した特定の宛先の送信メール等を他のアドレスに転送させる等の高度な盗聴行為に対しても有効に対抗することができる新規なパケット通信システム及びパケット通信方法を提供することを目的する。

【０００８】

【課題を解決するための手段】請求項１の発明に係るパケット通信方法は、網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザＩＤを抽出する工程と、上記正規のユーザＩＤと異なる任意のユーザＩＤを発生し、この任意のユーザＩＤを上記正規のユーザＩＤが抽出されたヘッダ中に挿入して新規のヘッダを生成する工程と、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザＩＤを挿入してパケットを組み立てる工程と、上記工程により組み立てられたパケットを送信する工程とを備えたものである。

【０００９】請求項２の発明に係るパケット通信方法は、上記送信パケットに暗号化処理又はスクランブル処理を施したものである。

【００１０】請求項３の発明に係るパケット通信方法は、網状の通信ネットワークに接続されたローカル通信ネットワーク内に設けられ、上記通信ネットワークに接続された他のローカル通信ネットワークとの間においてパケット化された通信データを送受信するサーバ装置と、このサーバ装置に接続され、上記サーバ装置に蓄積された自己宛の通信データの取り出し及び上記サーバ装置に対して生成した通信データの送信をそれぞれ行う複数の端末装置と、これら複数の端末装置からそれぞれ送信される通信データのパケットを編集し、そのパケットに付加された送信先の端末装置を示すアドレスのうちローカルアドレスに対応するユーザＩＤをパケット毎に書き替えて上記サーバ装置に出力し、かつ、上記サーバ装置から上記端末装置に取り出される通信データのパケットに付加されたローカルアドレスの識別を行い、自己が属するローカル通信ネットワークのローカルアドレス以外のローカルアドレスが付加されたパケットを蓄積し、蓄積した各パケットから正規のユーザＩＤを抽出したときは抽出した正規のユーザＩＤによりパケットを組立て直して当該ユーザＩＤの端末装置に出力し、上記正規のユーザＩＤを抽出できなかったときは上記蓄積したパケットを破棄するパケット編集手段とを備えたものである。

【００１１】

【発明の実施の形態】実施の形態１．以下、この発明の実施の形態１について図１乃至図３を用いて説明する。

4

図１はこの発明の実施の形態１によるパケット通信システムを示すシステム構成図であり、図１において、１は公衆通信網等の通信ネットワーク、２ａ，２ｂ及び２ｃは通信ネットワーク１に接続されたルータ、３ａ，３ｂは各ルータ２ａ，２ｂに接続されたファイアウォール、４ａ，４ｂは各ファイアウォール３ａ，３ｂに接続された組織のメールサーバ、５ａ，５ｂは組織のメールサーバ４ａ，４ｂに接続された所属元のメールサーバ、６ａ－１，６ａ－２，６ｂ－１，６ｂ－２は所属元のメールサーバ５ａ，５ｂにそれぞれ接続された個人又は共通用の端末装置、７ａ，７ｂは所属元のメールサーバ５ａ，５ｂにそれぞれ接続され、後述するようなパケットの編集を行うパケット編集手段である。なお、メールサーバ４ａ，４ｂ及び５ａ，５ｂはそれぞれ通信ネットワーク１上における電子郵便箱（ｍａｉｌ　ｂｏｘ）に相当する機能を提供するサーバであり、いわゆる電子メールの送受信処理を実行する。また、ルータ２ａ、２ｂ及び２ｃは通信ネットワーク１と各企業等に設けられたパケット通信システムとを接続するもので、これら各ルータ２ａ、２ｂ及び２ｃのＩＰアドレスが各ローカル通信ネットワークの宛先として通信ネットワーク１上に公開されている。

【００１２】次に動作についてさらに図２乃至図６を用いて説明する。図２は図１に示すパケット編集手段７ａ，７ｂの具体構成を示すブロック構成図、図３は図１に示すパケット通信システムの送信動作を説明するフローチャート図、図４は図１に示すパケット通信システムの送信動作を説明するフローチャート図である。なお、図１において、２ａ，３ａ，４ａ，５ａ，６ａ及び７ａは送信側のパケット通信システム、２ｂ，３ｂ，４ｂ，５ｂ，６ｂ及び７ｂは受信側のパケット通信システムを示し、それぞれ通信ネットワーク１に対してローカル通信ネットワークを構成しているものとする。また、この実施の形態では、送信側の端末装置６ａ－１から受信側の端末装置６ｂ－２に対して電子メールの送信を行う場合を例として説明する。

【００１３】例えば、送信側の端末装置６ａ－１において電子メールの作成が行われると、その電子メールはパケットと呼ばれる多数のデータに分割されて所属元のメールサーバ５ａに対して送出される。この端末装置６ａ－１から送出されたパケット（以下、送信パケットという）は所属元のメールサーバ５ａに出力される前にパケット編集手段７ａに取り込まれて送信パケットの編集処理が行われる。図２に示すように、パケット編集手段７（送受信の区別をしない場合は単にパケット編集手段７という。他の構成も同様であり、送受信の区別をしない場合はａ，ｂによる区別は行わない。）は送信処理部８及び受信処理部９をそれぞれ有しており、送信側のパケット通信システムにおける端末装置６ａ－１から創出された送信パケットは送信処理部８においてパケットの編

5

集処理が行われる。なお、受信側のパケット通信システムにおいて受信された電子メールは受信処理部９によりパケットの編集処理が行われるが、これについては後述する。以下、送信パケットの編集処理についてさらに図３を参照して詳細に説明する。

【００１４】端末装置６ａ－１から送出された送信パケットは、先ず送信処理部８のパケット選択部１０に取り込まれる（Ｓ０１）。パケット選択部１０に取り込まれた送信パケットはＩＤ抽出部１１によりパケットの再組み立てに必要な固有データが抽出された後、データ変換部１２に出力される（Ｓ０２）。ここで、固有データとは、送信パケットのヘッダ中に挿入された送信先の端末装置の内部アドレスを示すローカルアドレスに対応したユーザＩＤである。各送信パケットのヘッダには送信先のアドレス、送信元のアドレス、パケット順序等を示す各種の情報が挿入されているが、そのうちの送信先の端末装置、例えば端末装置６ｂ－１等の内部アドレスを示すローカルアドレスに対応したユーザＩＤが固有データとして抽出される。

【００１５】図５は端末装置６ａ－１等において作成された電子メールのイメージ図であり、図５において、２０はヘッダに挿入される情報部分、２１はデータ部に分割される情報部分、２２はヘッダ情報部２０、データ情報部２１の情報からなる電子メールである。図５に示すように、ヘッダ情報部２０は送信元のアドレス、送信先のアドレス、送信日時、件名等の情報を有しており、これらの情報が分割された送信パケットの各ヘッダに挿入される。そして、各パケットのヘッダ中に挿入された送信先のアドレスのうち、送信先の端末装置の内部アドレスを示すローカルアドレスに対応したユーザＩＤ（図５に示す送信先を示すアドレスであるｙｙｙｙ＠ｙｙｙ．ｙｙｙ．ｃｏ．ｊｐのうち、ｙｙｙｙの部分）の情報がＩＤ抽出部１１により抽出される。なお、このような電子メール２２の作成は各端末装置に設けられたメールソフト等を用いて作成することができる。

【００１６】また、１３はＩＤ抽出部１１により抽出された正規のユーザＩＤに代わる任意のユーザＩＤを発生する変換データ発生部であり、この変換データ発生部１３から出力されたヘッダ変換用のユーザＩＤがデータ変換部１２に出力される（Ｓ０３）。データ変換部１２にはパケット選択部１０において正規のユーザＩＤが抽出された後の各送信パケットが入力されており、変換データ発生部１３から出力されたヘッダ変換用のユーザＩＤにより新規のヘッダが生成される（Ｓ０４）。すなわち、端末装置６から送出された各送信パケットのヘッダが他のヘッダに変換されることになる。データ変換部１２によりヘッダの変換が行われた送信パケットは、パケット組立部１４に出力される。

【００１７】パケット組立部１４はデータ変換部１３によりヘッダの変換が行われた送信パケットが入力される

6

と、その送信パケットのデータ部の任意の位置にＩＤ抽出部１１により抽出された正規のユーザＩＤを挿入し、かつ、これらのデータが通信ネットワーク１の通信プロトコルに適合するようパケットの組立てを行って所属元のメールサーバ５ａに出力する。例えば、インターネットの場合、トランスポート層のプロトコルに適合させるパケットの組立てが行われる（Ｓ０５）。このように、パケット組立部１４ではパケット選択部１０に取り込まれた送信パケットとは異なる新たな送信パケットが組み立てられて所属元のメールサーバ５ａに対して出力される（Ｓ０６）。所属元のメールサーバ５ａに送出された各送信パケットは組織のメールサーバ４ａを経由して通信ネットワーク１にそれぞれ送出される。

【００１８】通信ネットワーク１に送出された各送信パケットには送信先のメールサーバの外部アドレス（例えば、図５に示す送信先を示すアドレスであるｙｙｙｙ＠ｙｙｙ．ｙｙｙ．ｃｏ．ｊｐのうち、ｙｙｙ．ｃｏ．ｊｐの部分）の情報が付与されており、通信ネットワーク１は各送信パケットに付与された送信先のメールサーバの外部アドレス、すなわちＩＰアドレスを参照しながら送信先の端末装置が属するメールサーバまで送信パケットを転送する。なお、図５に示す送信先を示すアドレスであるｙｙｙｙ＠ｙｙｙ．ｙｙｙ．ｃｏ．ｊｐのうち、＠ｙｙｙの部分は所属元のメールサーバのアドレス情報が付与された部分であり、この部分のアドレス情報により組織のメールサーバ４ｂから該当する所属元のメールサーバ５ｂに対して受信メールの転送が行われる。

【００１９】このように、パケット編集手段７ａはＩＰアドレスに該当する部分ではなく、ユーザＩＤの部分のデータを任意のデータに変換しているので、通信ネットワーク１に送出された送信パケットはヘッダ中に挿入された外部アドレスに従って送信先のメールサーバへ確実に送信される。なお、外部アドレスは変換していないので、送信先の端末装置６ｂ－２が属する組織のメールサーバ４ｂのアドレスを対象としたパケットフィルタリング等により送信パケットを捕捉されるおそれがあるが、たとえ送信パケットが捕捉されても、内部アドレスであるユーザＩＤが他のユーザＩＤ、例えば、存在しないユーザＩＤに変換されており、また、各送信パケットの相関関係が破棄されており、どの端末装置を宛先とする送信パケットであるか識別することはできず、いわゆるパケットフィルタリングによる盗聴行為を防止することができる。

【００２０】また、変換データ発生部１３から出力されるヘッダ変換用のユーザＩＤの種類には制限がないので、全くランダムにユーザＩＤを発生させることでき、変換データ発生部１３から出力されるヘッダ変換用のユーザＩＤをランダム化することにより各送信パケット間の相関関係を破棄することができる。これによりパケットフィルタリングによる盗聴行為をさらに困難とするこ

とができ、仮に全ての送信パケットが捕捉され同一性の解析等がなされても、送信した電子メールの内容が他人に知られるおそれは極めて低い。

【００２１】図６（ａ）は各端末装置６によりパケット化された送信パケットのデータ構成を示すデータ構成図、図６（ｂ）はパケット組立部１４において組み立てられた新たな送信パケットのデータ構成を示すデータ構成図である。図６（ｂ）に示すように、パケット組立部１４において組み立てられた新たな送信パケットには新規ヘッダ２３ｂが付与されると共に、データ部２４ｂに正規のユーザＩＤが挿入されている。このため、たとえ受信側メールサーバの処理プログラムを書き替えて受信側のメールサーバに到着した送信メールの内容を盗聴する行為、例えば、目的の送信パケットに記述された送信先アドレスを書き替えて特定のアドレスに転送させるような処理等がなされても、ヘッダ中に挿入された送信先の端末装置を示すユーザＩＤがランダム化されており、転送させる送信パケットの識別自体を行うことができず、このような盗聴行為に対しても有効に対抗することができる。なお、後述するように、受信側ネットワークのパケット編集手段７ｂでは、受信パケットを図６（ｂ）に示すパケット状態から図６（ａ）に示す状態に戻す編集処理が行われる。

【００２２】次に受信動作について説明する。上述したとおり、送信側ネットワークのパケット編集手段７ａを介して通信ネットワーク１に送出された送信パケットは、送信パケットのヘッダ中に挿入された送信先の外部アドレスが参照されて送信先である端末装置が属する受信側ネットワークのルータ２ｂに転送され、ファイアウォール３ｂ、組織のメールサーバ４ｂを経由して所属元のメールサーバ５ｂに転送される。図５に示すようなメールアドレスは、通常、ローカル通信ネットワークの内部アドレスを示すユーザＩＤとその外部アドレスを示すＤＮＳ（ｄｏｍａｉｎ　ｎａｍｅ　ｓｙｓｔｅｍ）の部分で構成されており、ＤＮＳの部分は通信ネットワーク１内を転送される際に参照されるＩＰアドレスと関連付けされていることから変更することができないが、ユーザＩＤは通信ネットワーク１内における転送に関与しておらず、自由に変更することできる。

【００２３】この実施の形態１によるパケット通信システムでは、送信パケットのヘッダ中に挿入された送信先のアドレスのうち、ユーザＩＤの部分のアドレス情報のみが編集され他の部分は正規のアドレス情報のままであるので、受信側ネットワークのルータ２ｂに到達した送信パケットはその送信先の端末装置が属する所属元のメールサーバ５ｂまで確実に転送することができる。

【００２４】なお、パケット編集手段７ｂを設ける位置によって、パケット編集手段７におけるヘッダ変換の対象を変更することができ、組織のメールサーバ４ｂと所属元のメールサーバ５ｂとの間にパケット編集手段７を設ける場合には、組織のメールサーバ４ｂまで受信パケットの転送が行われればよく、図５に示す送信先を示すアドレスであるｙｙｙｙ＠ｙｙｙ．ｙｙｙ．ｃｏ．ｊｐのうち、ｙｙｙｙ＠ｙｙｙの部分のアドレス情報をパケット編集手段７におけるヘッダ変換の対象とすることができる。但し、ネットワークの上位にパケット編集手段７ｂを配置すると、その下位に接続されている全ての端末装置のパケット編集を負担しなければならず、処理負担を分散させる観点からネットワークの下位、例えば、所属元のメールサーバ毎、あるいは高度の盗聴防止機能が要求される端末装置群が属する所属元のメールサーバ５ｂのみを対象としてパケット編集手段７を配置することが望ましい。

【００２５】所属元のメールサーバ５ｂに転送されたパケット（以下、受信パケットという）はヘッダ中に挿入されたユーザＩＤが他のユーザＩＤに変換されており、そのままではどの端末装置に対して送信されたパケットであるかを識別することができず、送信先の端末装置６ｂ－２が所属元のメールサーバ５ｂに対してその受信メールの読出しを要求してもその受信パケットを送信先の端末装置６ｂ－２に対して転送することはできない。そこで、所属元のメールサーバ５ｂに転送された受信パケットはパケット編集段７ｂにより受信パケットの編集が行われる。上述したように、パケット編集手段７は送信処理部８及び受信処理部９をそれぞれ有しており、受信側ネットワークにおいて受信された受信パケットは受信処理部９において受信パケットの編集処理が行われる。以下、受信パケットの編集処理についてさらに図４を参照して詳細に説明する。

【００２６】送信側のネットワークのパケット編集手段７ａにおいてパケットの編集処理が行われた受信パケットは、まずパケット取得部１５により取り込まれる（Ｓ０７）。パケット取得部１５により取得された受信パケットはパケット識別部１６により対象とするパケットであるか否かが識別される（Ｓ０８）。受信パケットのヘッダ中には送信先のアドレスが挿入されており、同一の送信先のパケットには同一のアドレスが挿入されているが、この実施の形態１によるパケット通信システムでは、送信パケットのヘッダ中に挿入された送信先のアドレス情報のうちユーザＩＤの部分のアドレス情報を他のユーザＩＤに変換しているので、対象となる受信パケットにおけるユーザＩＤはその受信側ネットワークには存在しないユーザＩＤ又は同一のユーザＩＤがないものとなっており、そのようなユーザＩＤを有する受信パケットは本発明に係るパケットの編集処理がなされた対象パケットであると判断して対象パケット蓄積部１８に蓄積する（Ｓ０９）。

【００２７】また、通常、受信パケットは受信側のいメールサーバ５ｂから各端末装置への転送において、ＭＡＣアドレス（マシンアドレス）が参照されるが、送信側

のパケット編集手段７ａによるパケットの編集処理が行われた受信パケットはユーザＩＤとＭＡＣアドレスとが一致しないことから、エラーと認識され廃棄や送信元への返信等が行われる。しかし、この実施の形態によるパケット通信システムでは、このようなエラーと認定される受信パケットのうちパケット編集手段７ｂの送信処置部８においてパケットの編集処理が行われたパケットを蓄積し受信パケットの再組立て処理を実行する。なお、パケット識別部１６により対象パケットでないと判断された受信パケットはパケット編集手段７によるパケットの編集処理がなされていないものと予想されるため、このような受信パケットについてはパケット破棄部１７に出力され自動破棄される（Ｓ１０）。

【００２８】対象パケット蓄積部１８に蓄積された受信パケットは、正規のユーザＩＤに基づくパケットの再組立てを行うべく、パケット再組立部１９に送られる。パケット再組立部１９は、まず対象パケット蓄積部１７に蓄積された受信パケットのヘッダ中に挿入された送信先のアドレス情報のうち、ユーザＩＤに関する情報を削除する。そして、その受信パケットのデータ部に挿入されている正規のユーザＩＤを抽出し（Ｓ１１）、この正規のユーザＩＤを受信パケットのヘッダ中に挿入することにより受信パケットの再組立てを行う（Ｓ１２）。パケット再組立部１９は対象パケット蓄積部１８に蓄積された全ての受信パケットについてこのようなパケットの再組立てを行い、送信元の端末装置６ａ－１から送出された全ての送信パケットがこのようなパケットの再組立てにより元のパケット状態に戻され所属元のメールサーバ５ｂに対して出力される（Ｓ１３）。

【００２９】このように、パケット再組立部１９により組み立てられた受信パケットのヘッダ中には送信先の端末装置６ｂ－２の内部アドレスを示す正規のユーザＩＤが挿入されており、また、所属元のメールサーバ５ｂは接続されている各端末装置６ｂ－１，６ｂ－２等の内部アドレスを全て把握しているので、受信パケットがどの端末装置に対して送信されたパケットであるかを識別することができ、端末装置６ｂ－２から受信メールの読出しの要求があった場合に送信側ネットワークの端末装置６ａ－１から送信された送信メールの内容を確実に送信先の端末装置６ｂ－２に対して転送させることができる。

【００３０】なお、この実施の形態１によるパケット通信方法及びパケット通信システムにおいて、送信パケットの暗号化処理やスクランブル処理等を併用するように構成してもよい。この場合、さらにデータの保全効果を向上させることができる。また、この実施の形態１によるパケット通信方法及びパケット通信システムは、電子メールデータの送受信を行うものであるが、データをパケット化して送受信する方式のものであれば、データの種類・内容に関係なく適用することが可能であり、メールサーバのように受信したパケットデータを蓄積し端末装置から取り出すように構成された他のシステムにも適用することができる。

【００３１】

【発明の効果】以上のように、請求項１に係る発明によれば、網状の通信ネットワークを経由してパケット化された通信データを送受信するパケット通信方法において、上記パケットに付加されたヘッダ中の送信先を示すアドレスのうち、上記送信先が属するローカル通信ネットワークの内部アドレスであるローカルアドレスに対応する正規のユーザＩＤを抽出する工程と、上記正規のユーザＩＤと異なる任意のユーザＩＤを発生し、この任意のユーザＩＤを上記正規のユーザＩＤが抽出されたヘッダ中に挿入して新規のヘッダを生成する工程と、この新規のヘッダを上記パケットのデータ部分に付加すると共に、このデータ部分に上記抽出された正規のユーザＩＤを挿入してパケットを組み立てる工程と、上記工程により組み立てられたパケットを送信する工程とを設けたので、タッピング等のネットワーク経路上において行われる盗聴行為、さらには受信側のサーバに侵入し、受信側サーバの処理プログラムを書き替えて受信側サーバに到着した特定の宛先の送信メール等を他のアドレスに転送させる等の高度な盗聴行為に対しても有効に対抗することができる。

【００３２】また、暗号処理又はスクランブル処理を併用することにより、さらにデータの保全効果を向上させることができる。

【図面の簡単な説明】

【図１】　この発明の実施の形態１によるパケット通信システムを示すシステム構成図である。

【図２】　図１に示すパケット編集手段７ａ，７ｂの具体構成を示すブロック構成図である。

【図３】　図１に示すパケット通信システムの送信動作を説明するフローチャート図である。

【図４】　図１に示すパケット通信システムの送受信動作を説明するフローチャート図である。

【図５】　端末装置６ａ－１、６ｂ－１等において作成された電子メールのイメージ図である。

【図６】　図１に示す端末装置６ａ－１等によりパケット化された送信パケットのデータ構成及びパケット編集手段７ａ等によりパケットの編集が行われた新たなパケットのデータ構成を示すデータ構成図である。

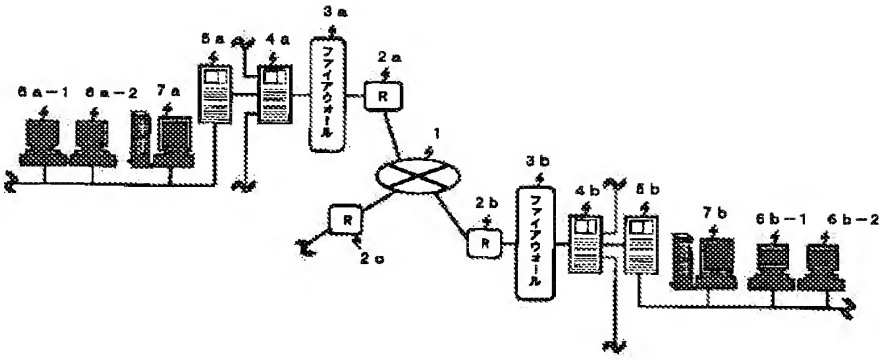
【符号の説明】

１　通信ネットワーク
２，２ａ，２ｂ　ルータ
３，３ａ、３ｂ　ファイアウォール
４，４ａ，４ｂ　サーバ装置（組織のメールサーバ）
５，５ａ，５ｂ　サーバ装置（所属元のメールサーバ）
６，６ａ－１，６ａ－２，６ｂ－１，６ｂ－２　端末装置

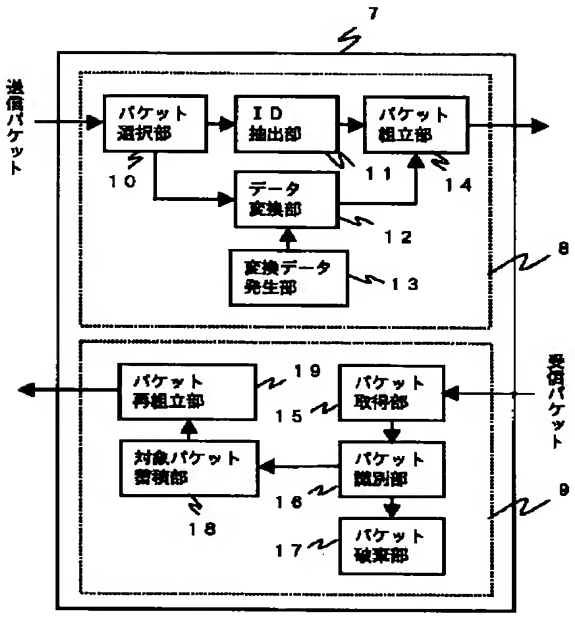
11　　12

７，７ａ，７ｂ　パケット編集手段。

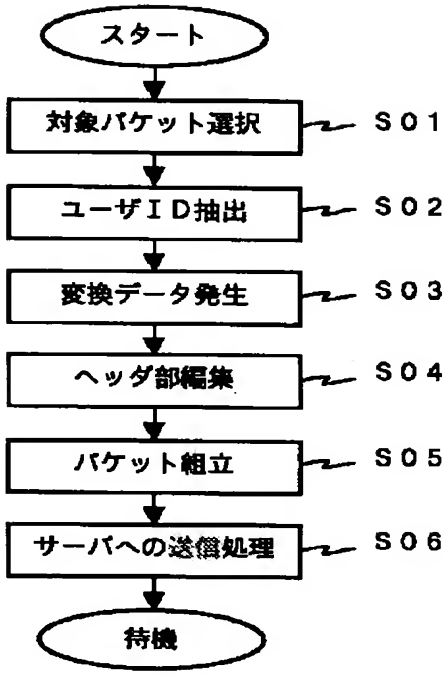
【図１】



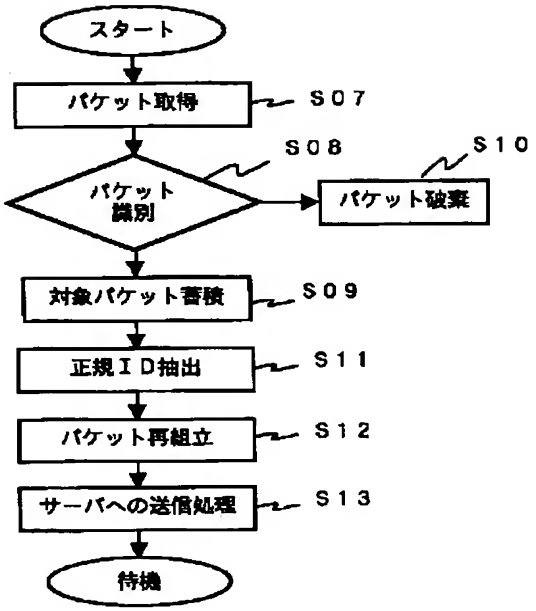
【図２】



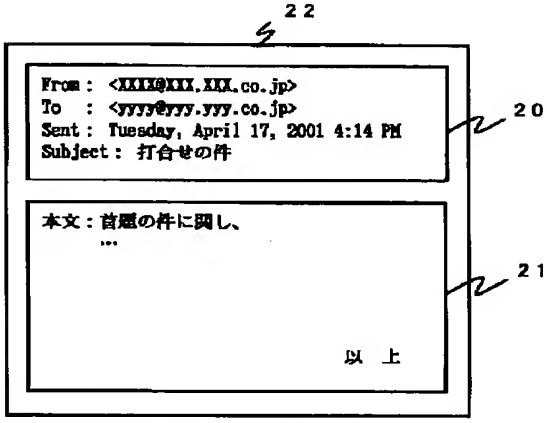
【図３】



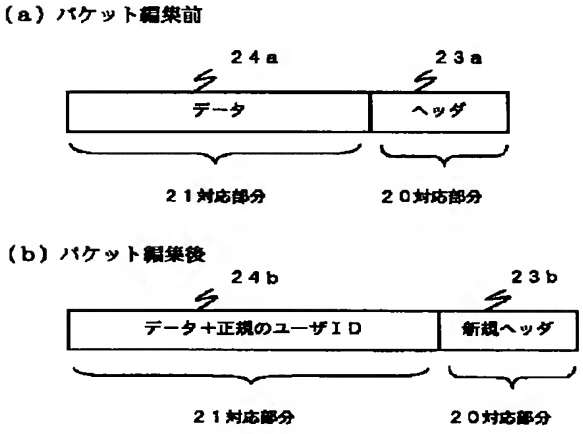
【図４】



【図５】



【図６】



フロントページの続き

Ｆターム(参考) 5J104 AA04 AA07 BA06 KA02 NA02
PA08
5K030 GA15 HA07 HB21 HC01 HC14
HD07 JA05 JA11 KA04 KA06
KX24 LB16 LC18 LD19 LE12
MB18